Amendments to the Claims

This listing of claims will replace all prior versions and listings of claims in the application:

Listing of Claims

Claim 1 (Currently amended): A communication system having a server for providing a Web E-mail service to a Web browser of a client, wherein said server comprises:

management means for managing a secret key for decrypting an encrypted E-mail message addressed to a user's mail address, the E-mail message being encrypted by a public key corresponding to the user's mail address, wherein the secret key corresponding to the user's mail address for decrypting the encrypted E-mail message is not managed by the Web browser of the client;

web encryption communication means for establishing a Web encryption communication with the Web browser of the client, and communicating with the Web browser of the client by the Web encryption communication established by said web encryption communication means;

authentication means for executing authentication of a use allowance of the secret key managed by said management means to the Web browser of the client when the Web browser of the client requests to decrypt the encrypted E-mail message while the server communicates with the client by said established Web encryption communication;

decrypting means for making a decrypted E-mail message by decrypting the encrypted E-mail message using the secret key managed by said management means, the secret key corresponding to the user's mail address, in the case where the use allowance of the secret key managed by said management means is authenticated by said authentication means; and

transmission control means for controlling to transmit the decrypted E-mail message decrypted by said decrypting means to the client through the Web encryption communication established by said web encryption communication means, the decrypted E-mail message being not re-encrypted by a public key when the decrypted E-mail message is transmitted by said transmission control means.

Claim 2 (Cancelled)

Claim 3 (Previously presented): The communication system according to claim 1, wherein said authentication means provides said client with a window data to authenticate the use allowance of the managed key.

Claim 4 (Previously presented): The communication system according to claim 1, wherein said authentication means authenticates the use allowance using a passphrase inputted from said client.

Claim 5 (Previously presented): The communication system according to claim 1, wherein said authentication means authenticates the use allowance based on a biometrics information of a user inputted from said client.

Claim 6 (Previously presented): The communication system according to claim 1, wherein said web encryption communication means establishes the Web encryption communication with the client by using SSL.

Claim 7 (Cancelled).

Claim 8 (Previously presented): The communication system according to claim 1, wherein said authentication means authenticates the use allowance of the managed key during a session of the Web encryption communication continuously established between said client and a server.

Claim 9 (Previously presented): The communication system according to claim 8, wherein said authentication means stops said authenticated use allowance, in the case where at least either the case where the Web encryption communication is ended with an error or the case where the Web encryption communication has passed a fixed time is satisfied.

Claim 10 (Previously presented): The communication system according to claim 1, wherein said server further comprises signature means for executing a digital signature to an E-mail created by said client.

Claim 11 (Previously presented): The communication system according to claim 1, wherein said server further comprises:

multiple use judging means for judging whether the managed key is under multiple use, and

stop means for stopping the use allowance of a session under multiple use in the case where the session is judged to be under multiple use by said multiple use judging means.

Claim 12 (Previously presented): The communication system according to claim 1, wherein the key for decrypting the encrypted E-mail is a secret key in a code of a public key cryptosystem.

Claim 13 (Currently amended): A communication system having a client receiving a Web E-mail service from a server, wherein the server comprises:

management means for managing a secret key for decrypting an encrypted E-mail message addressed to a user's mail address, the E-mail message being encrypted by a public key corresponding to the user's mail address, wherein the secret key corresponding to the user's mail address for decrypting the encrypted E-mail message is not managed by the Web browser of the client;

web encryption communication means for establishing a Web encryption communication with the Web browser of the client, and communicating with the Web browser of the client by the Web encryption communication established by said web encryption communication means;

authentication means for executing authentication of a use allowance of the secret key managed by said management means to the Web browser of the client based on authentication information sent from the client when the Web browser of the client requests to decrypt the encrypted E-mail message while the server communicates with the client by the established Web encryption communication;

decrypting means for making a decrypted E-mail message by decrypting the encrypted E-mail message using the secret key managed by said management means, the secret key corresponding to the user's mail address, in the case where the use allowance of the secret key managed by said management means is authenticated by said authentication means, the decrypted E-mail message being not re-encrypted by a public key when the decrypted E-mail message is transmitted by said transmission control means; and

transmission control means for controlling to transmit the decrypted E-mail message decrypted by said decrypting means to the client through the Web encryption communication established by said Web encryption communication means, and

wherein the client comprises:

request means for requesting to decrypt the encrypted E-mail message while said Web encryption communication is established between the server and the Web browser of the client;

authentication information sending means for sending the authentication information to said authentication means; and

receiving means for receiving the decrypted E-mail message transmitted by said transmission control means through the Web encryption communication established by said Web encryption communication means.

Claim 14 (Currently amended): A method for controlling a communication system including a server for providing a Web browser of a client with a Web E-mail service, comprising:

a management step of managing a secret key for decrypting an encrypted E-mail message addressed to a user's mail address, the E-mail message being encrypted by a public key corresponding to the user's mail address, wherein the secret key corresponding to the user's mail address for decrypting the encrypted E-mail message is not managed by the Web browser of the client;

a web encryption communication step for establishing a Web encryption communication with the Web browser of the client, and communicating with the Web browser of the client by the Web encryption communication established in said web encryption communication step;

an authentication step of executing authentication of a use allowance of the secret key managed in said management step to the Web browser of the client when the Web browser of the client requests to decrypt the encrypted email message while the server communicates with the client by said established Web encryption communication;

a decrypting step of making a decrypted E-mail message by decrypting the encrypted E-mail message using the secret key managed in said management step, the secret key corresponding to the user's mail address, in the case where the use allowance of the secret key managed in said management step is authenticated in said authentication step, the decrypted E-mail message being not re-encrypted by a public key when the decrypted E-mail message is

transmitted in said transmission control step; and

a transmission control step of controlling to transmit the decrypted E-mail message decrypted in said decrypting step to the client through the Web encryption communication established in the web encryption communication step.

Claim 15 (Cancelled)

Claim 16 (Previously presented): A method for controlling the communication system according to claim 14, wherein, in said authentication step, a window data for authenticating the use allowance of the managed key is supplied to said client for authentication.

Claim 17 (Previously presented): A method for controlling the communication system according to claim 14, wherein, in said authentication step, the use allowance is authenticated using a passphrase inputted from said client.

Claim 18 (Previously presented): A method for controlling the communication system according to claim 14, wherein, in said authentication step, the use allowance is authenticated based on biometrics information of a user inputted from said client.

Claim 19 (Previously presented): A method for controlling the communication system according to claim 14, wherein, in said server, said web encryption communication step establishes the Web encryption communication with the client by using SSL.

Claim 20 (Cancelled).

Claim 21 (Previously presented): A method for controlling the communication system according to claim 14, wherein, in said authentication step, the use allowance of the managed key is authenticated during a session of the Web encryption communication continuously established between said client and a server.

Claim 22 (Previously presented): A method for controlling the communication system

according to claim 21, wherein, in said authentication step, said authenticated use allowance is stopped in the case when at least either the case where the Web encryption communication is ended with an error or the case where the Web encryption communication has passed a fixed time is satisfied.

Claim 23 (Previously presented): A method for controlling the communication system according to claim 14, further comprising a signature step of executing the digital signature to the E-mail created by said client in said server.

Claim 24 (Previously presented): A method for controlling the communication system according to claim 14, further comprising a step of executing a multiple use judging step of judging whether the managed key is under multiple use in the server, and a stop step of stopping the use allowance of a session under multiple use in the case where the session is judged to be under multiple use in said multiple use judging step.

Claim 25 (Previously presented): A method for controlling the communication system according to claim 14, wherein the key for decrypting the encrypted E-mail is a secret key in an encryption of a public key cryptosystem.

Claim 26 (Currently amended): A method for controlling a communication system including a client receiving a Web E-mail service from a server, comprising:

a step of executing a management step of managing a secret key for decrypting an encrypted E-mail message addressed to a user's mail address, the E-mail message being encrypted by a public key corresponding to the user's mail address, wherein the secret key corresponding to the user's mail address for decrypting the encrypted E-mail message is not managed by the Web browser of the client,

a web encryption communication step for establishing a Web encryption communication with the Web browser of the client, and communicating with the Web browser of the client by the Web encryption communication established in said web encryption communication step,

an authentication step of executing authentication of a use allowance of the secret key managed in said management step to the Web browser of the client based on authentication information sent from said client when the Web browser of the client requests to decrypt the encrypted E-mail message while the server communicates with the client by the established Web encryption communication,

a decrypting step of making a decrypted E-mail message by decrypting the encrypted E-mail message using the secret key managed in said management step, the secret key corresponding to the user's mail address, in the case where the use allowance of the secret key managed in said management step is authenticated in said authentication step, and

a transmission control step of controlling to transmit the decrypted E-mail message decrypted in said decrypting step to the client through the Web encryption communication established in said web encryption communication step, the decrypted E-mail message being not re-encrypted by a public key when the decrypted E-mail message is transmitted in said transmission control step,

wherein the client comprises:

a requesting step of requesting to decrypt the encrypted E-mail message while said Web encryption communication is established between the server and the Web browser of the client,

an authentication information sending step of sending the authentication information for authentication in said authentication step, and

a receiving step of receiving the decrypted E-mail message transmitted in said transmission step to the client through the Web encryption communication established in the web encryption communication step.

Claim 27 (Currently amended): A computer executable control program of a communication system including a server for providing a Web E-mail service to a Web browser of a client, said program comprising a management step of managing a secret key for decrypting an encrypted E-mail message addressed to a user's mail address, the E-mail message being encrypted by a public key corresponding to the user's mail address, wherein the secret key corresponding to the user's mail address for decrypting the encrypted E-mail message is not managed by the Web browser of the client, a web encryption communication step for establishing a Web encryption communication with the Web browser of the client, and communicating with the Web browser of the client by the Web encryption communication established in said web encryption communication step, an authentication step of executing authentication of a use allowance of the secret key managed in said management step to the Web browser of the client when the Web browser of the client requests to decrypt the encrypted E-mail message while the server communicates with the client by said established Web encryption communication, a decrypting step of making a decrypted E-mail message by decrypting the encrypted E-mail message using the secret key managed in said management step, the secret key corresponding to the user's mail address, in the case where the use allowance of the secret key managed in said management step is authenticated in said authentication step, and a transmission control step of controlling to transmit the decrypted E-mail message decrypted in said decrypting step to the client through the Web encryption communication established in said web encryption

communication step, the decrypted E-mail message being not re-encrypted by a public key when the decrypted E-mail message is transmitted in said transmission control step.

Claim 28 (Currently amended): A control program of a communication system including a client receiving a Web E-mail service through a Web from a server, comprising a step of executing a management step of managing a secret key for decrypting an encrypted E-mail message addressed to a user's mail address, the E-mail message being encrypted by a public key corresponding to the user's mail address, wherein the secret key corresponding to the user's mail address for decrypting the encrypted E-mail message is not managed by the Web browser of the client, a web encryption communication step for establishing a Web encryption communication with the Web browser of the client, and communicating with the Web browser of the client by the Web encryption communication established in said web encryption communication step, an authentication step of executing authentication of a use allowance of the secret key managed in said management step to the Web browser of the client based on authentication information sent from the client when the Web browser of the client requests to decrypt the encrypted E-mail message while the server communicates with the client by the established Web encryption communication, a decrypting step of making a decrypted E-mail message by decrypting the encrypted E-mail message using the secret key managed in said management step, the secret key corresponding to the user's mail address, in the case where the use allowance of the secret key managed in said management step is authenticated in said authentication step, and a transmission step of controlling to transmit the decrypted E-mail message decrypted in said decrypting step to the client through the Web encryption communication established in the web encryption communication step, the decrypted E-mail message being not re-encrypted by a public key when the decrypted E-mail message is

transmitted in said transmission step, and the client comprising a requesting step of requesting to decrypt the encrypted E-mail message while said Web encryption communication is established between the server and the Web browser of the client, an authentication information sending step of sending the authentication information for authentication in said authentication step, and a receiving step of receiving the decrypted E-mail message transmitted in said transmission step to the client through the Web encryption communication established in said web encryption communication step.

Claim 29 (Currently Amended): A storage medium storing a computer executable control program of a communication system including a server of providing a Web E-mail service to a Web browser of a client, the program comprising a step of executing a management step of managing a secret key for decrypting said encrypted E-mail message addressed to a user's mail address using said secret key, the E-mail message being encrypted by a public key corresponding to the user's mail address, wherein the secret key corresponding to the user's mail address for decrypting the encrypted E-mail message is not managed by the Web browser of the client, a web encryption communication step of establishing a Web encryption communication with the Web browser of the client, and communicating with the Web browser of the client by the Web encryption communication established in said web encryption communication step, an authentication step of executing authentication of a use allowance of the secret key managed in said management step to the Web browser of the client when the Web browser of the client requests to decrypt the encrypted E-mail message while the server communicates with the client by said established Web encryption communication, and a transmission control step of controlling to transmit the decrypted E-mail message to the client through the Web encryption communication established in said web encryption communication

step, the decrypted E-mail message being not re-encrypted by a public key when the decrypted E-mail message is transmitted in said transmission control step.

Claim 30 (Currently amended): A storage medium storing a control program of a communication system including a client receiving a Web E-mail service through a Web from a server, wherein the program comprises a step of executing a management step of managing a secret key for decrypting an encrypted E-mail message addressed to a user's mail address, the E-mail message being encrypted by a public key corresponding to the user's mail address, wherein the secret key corresponding to the user's mail address for decrypting the encrypted E-mail message is not managed by the Web browser of the client, a web encryption communication step of establishing a Web encryption communication with the Web browser of the client, and communicating with the Web browser of the client by the Web encryption communication established in said web encryption communication step, an authentication step of executing authentication of a use allowance of the secret key managed in said management step to the Web browser of the client based on authentication information sent from the client when the Web browser of the client requests to decrypt the encrypted E-mail message while the server communicates with the client by said established Web encryption communication, a decrypting step of making a decrypted E-mail message by decrypting the encrypted E-mail message using the secret key managed in said management step in the server, the secret key corresponding to the user's mail address, in the case where the use allowance of the secret key managed in said management step is authenticated in said authentication step, and a transmission control step of controlling to transmit the decrypted E-mail message decrypted in said decrypting step to the client through the Web encryption communication established in said web encryption communication step, the decrypted E-mail message being not re-encrypted

by a public key when the decrypted E-mail message is transmitted in said transmission control step, the client comprising a requesting step of requesting to decrypt the encrypted E-mail message while said Web encryption communication is established between the server and the Web browser of the client, an authentication information sending step of sending the authentication information for authentication in said authentication step, and a receiving step of receiving the decrypted E-mail message transmitted in said transmission step to the client through the Web encryption communication established in said web encryption communication step.